

Что такое
информационная
безопасность

Информация – это актив,
который имеет ценность.

ГОСТ Р ИСО/МЭК 17799 - 2005

Основные задачи ИБ

Обеспечение

- Конфиденциальности
- Целостности
- Доступности

информационных ресурсов

Проблемы, решаемые криптографией

- конфиденциальность
- целостность
- аутентификация
- невозможность отказа от авторства

Виды шифрования

Симметричное

- Общие или легко связываемые ключи шифрования
- Типичные длины ключей 128-256 бит

Ассиметричное

- Различные, неочевидно связанные ключи для шифрования
- Типичные длины ключей: 1024-4096 для операций в конечном поле, 256 бит для операций на эллиптической кривой

Принцип Керкхоффа

Надежность системы шифрования не должна основываться на ее секретности. Система должна оставаться надежной даже если все ее компоненты, кроме ключа стали известны атакующему.



Симметричные шифры

Типы симметричных шифров

Блочные

- Шифруется блок данных
- Типичный размер блока - 64 или 128 бит

Потоковые

- Генерируется поток псевдослучайных данных, зависящих от ключа
- Выход - поток бит (или байт), называемый *гаммой* - складывается по модулю с потоком данных

Шифры ПОДСТАНОВКИ

- Табличная подстановка
- Шифр Цезаря
 - Методика взлома
- Полиалфавитные шифры подстановки
- Шифр Виженера

Гай Юлий Цезарь

(12 июля 100 до н.э. –

15 марта 44 до н.э.)



Шифры перестановки

- Простая перестановка
- Перестановка по ключу



Антон Отто Фишер
«Горящий танкер»



Bletchley park

A vintage typewriter is shown inside its open, light-colored wooden carrying case. The typewriter has a dark body with a keyboard featuring light-colored keys. The interior of the case lid is a contrasting dark color and features a circular logo at the top and a horizontal slot in the center. The entire unit is placed on a dark, polished wooden surface. To the right, a portion of another museum display, a white card with a photograph, is visible.

This machine, marked in English, "Made in Germany", was intended for commercial export. Such Enigmas were available to anyone who wished to purchase them prior to the NAZI takeover of the German government.

[illegible][illegible]

THE PRINCIPLES

Following are the principles which the Government of the United States and the Government of the United Kingdom have agreed upon in the course of their negotiations for the purpose of establishing a permanent basis for the relations between the two countries.

1. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of friendship and cooperation between the two countries.

2. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of each other.

3. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the people of each country.

4. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the world.

5. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the future generations.

6. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the environment.

7. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the human race.

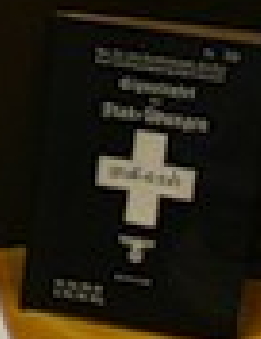
8. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the world community.

9. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the world peace.

10. The Government of the United States and the Government of the United Kingdom are determined to maintain the highest degree of respect for the rights and interests of the world order.

A commercial type machine specially wired. Five hundred of these Enigmas were given to the Japanese Navy for joint communications.

A specially constructed machine supplied to some foreign governments friendly to Germany. Two hundred "G" engines are known to have been issued to the German Army High Command (OKW) for an unknown "special purpose".



1827 3225XM C1626 W987

SEXTO

101
JUN 1968

H6R 5RH DE C 1346 = 3TLE = 2TL 224 = HUW XNG =

RE J

DKRKI CUZAF MNSDC AWXVJ DVZNH DMOZN NWRJC KKJQO

SNZ

ELWIK XDUUF ECEGN OUNNQ CIIZX FUTOG BTNWI GOECK

CMYUC KTTYB ZMDTU WCNWH OXOFX ERVQW JUCVY PQACQ

EBMXE NOQKF LWRWR LGKXZ BPYWR GQVYG WJDGA QXKVC

(Y)

MQQJJ PVSLG WFZJZ HHWQG YFCQQ RMVRR QQIDQ QVVIW

LJLBH LHHD1 OFWUY JJQGX BWPZ

CCT 2/3 RC%GN

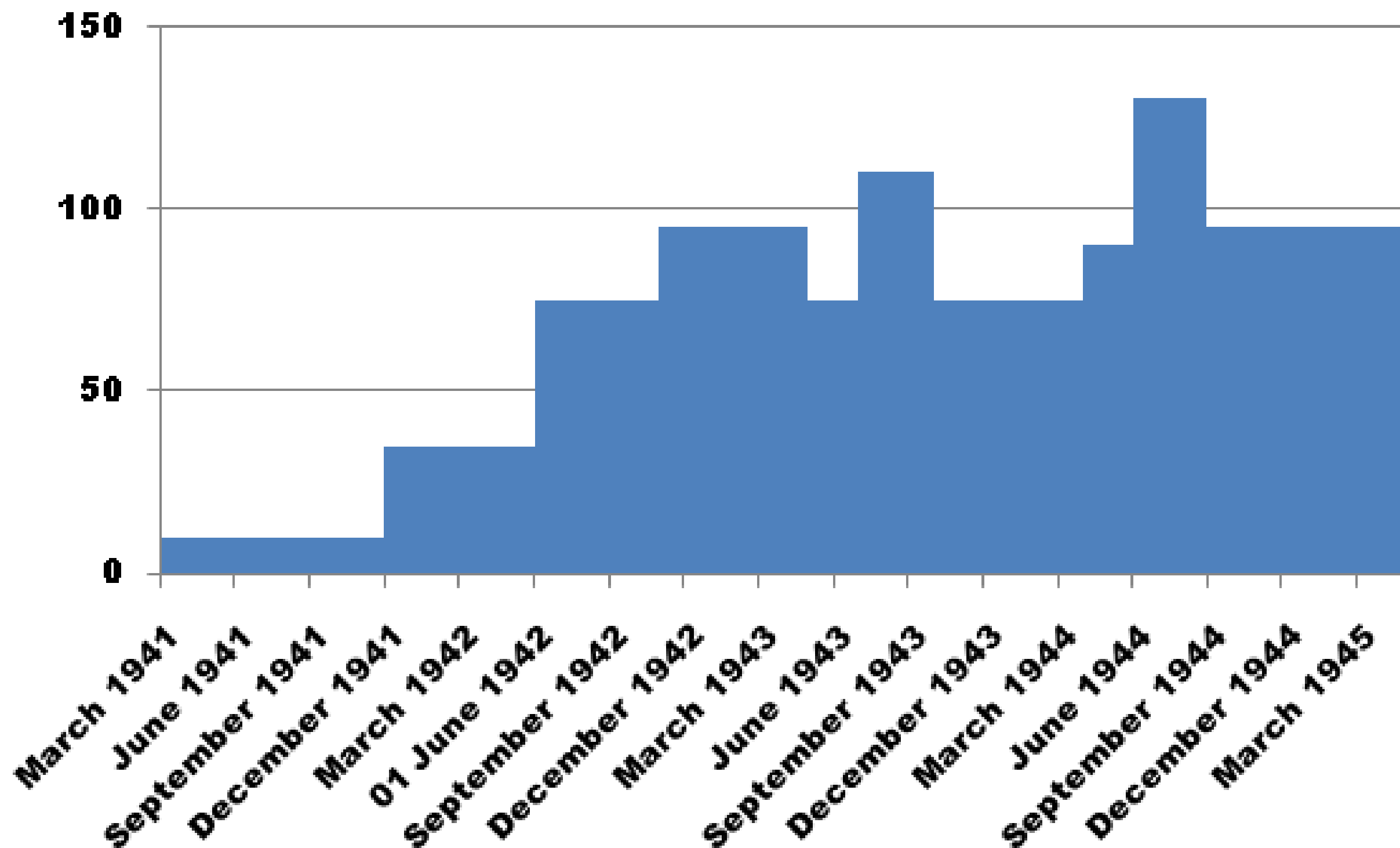
1852 FLC

**Алан
Тьюринг**



PHOENIX

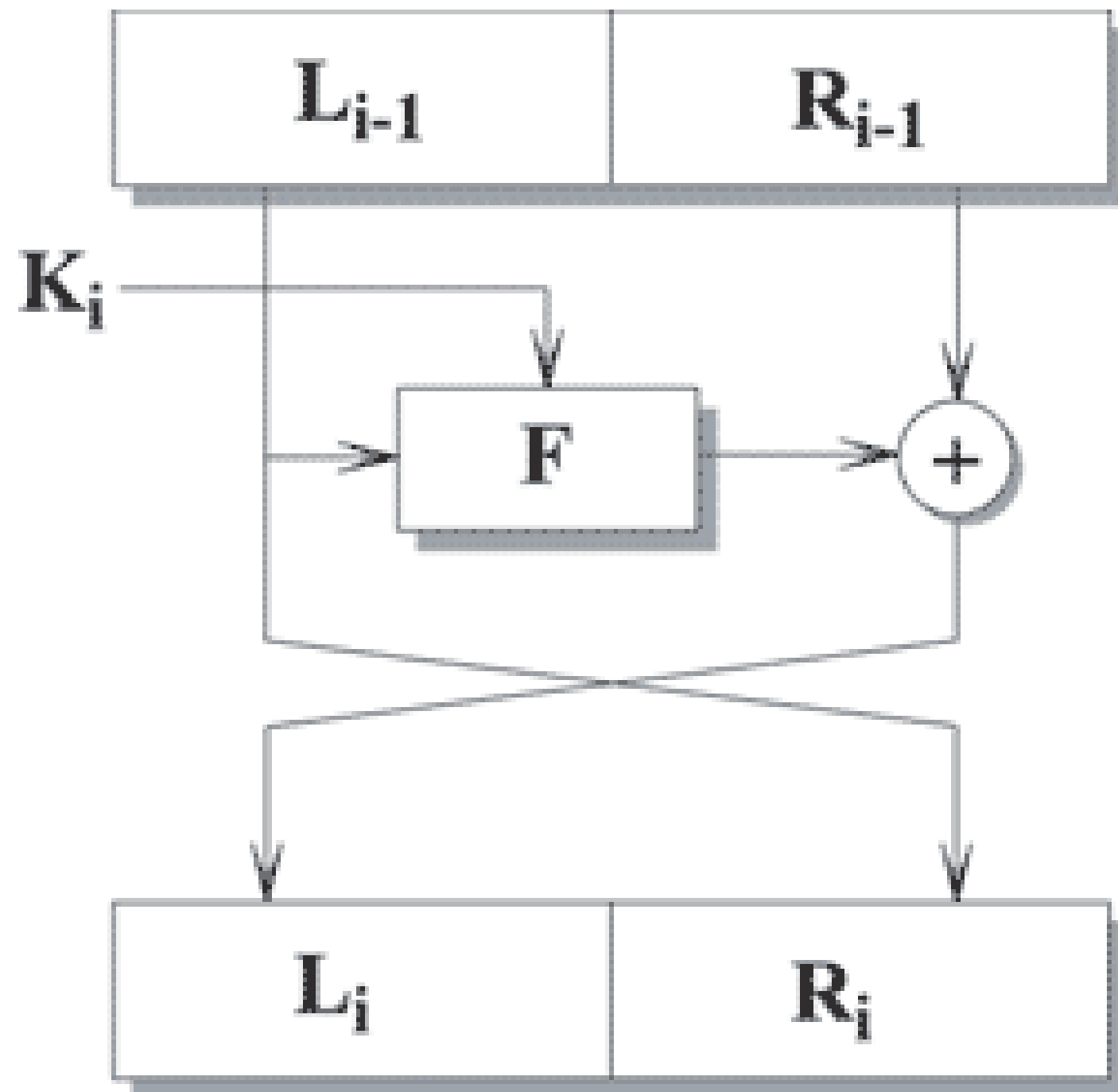




U-848

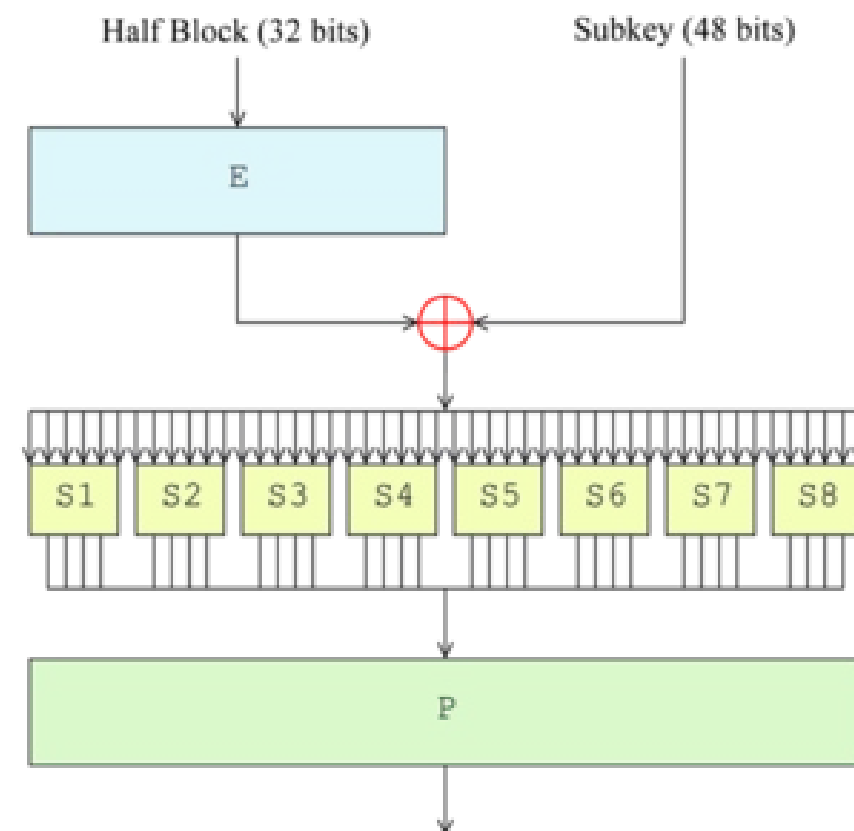


Сеть Фейстеля



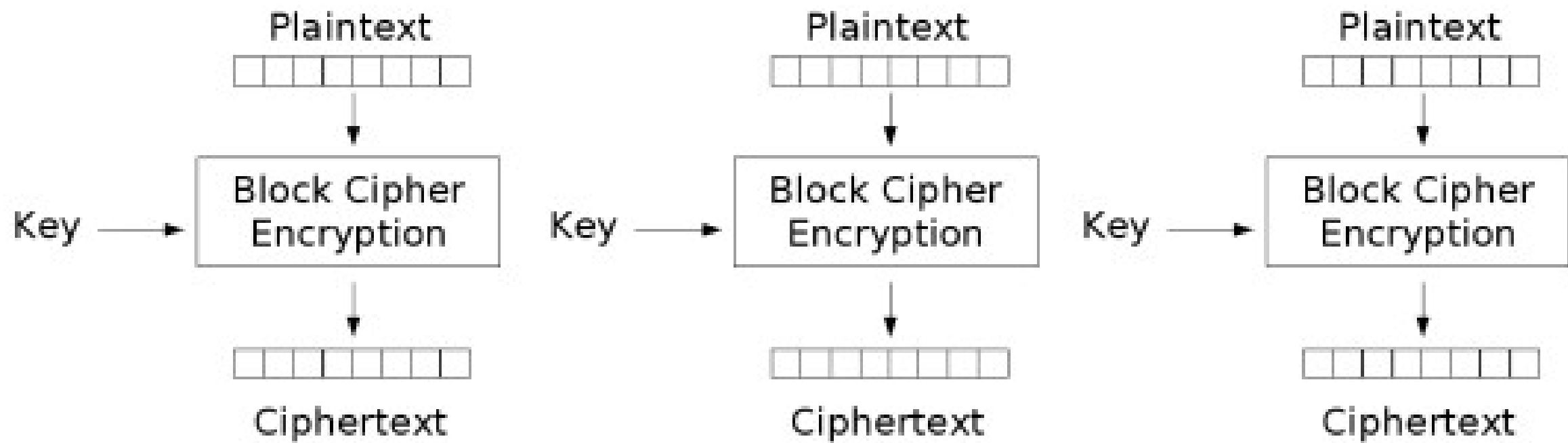
DES

- Сеть Фейстеля
- Размер блока - 64 бита
- Размер ключа - 56 бит
- 16 раундов



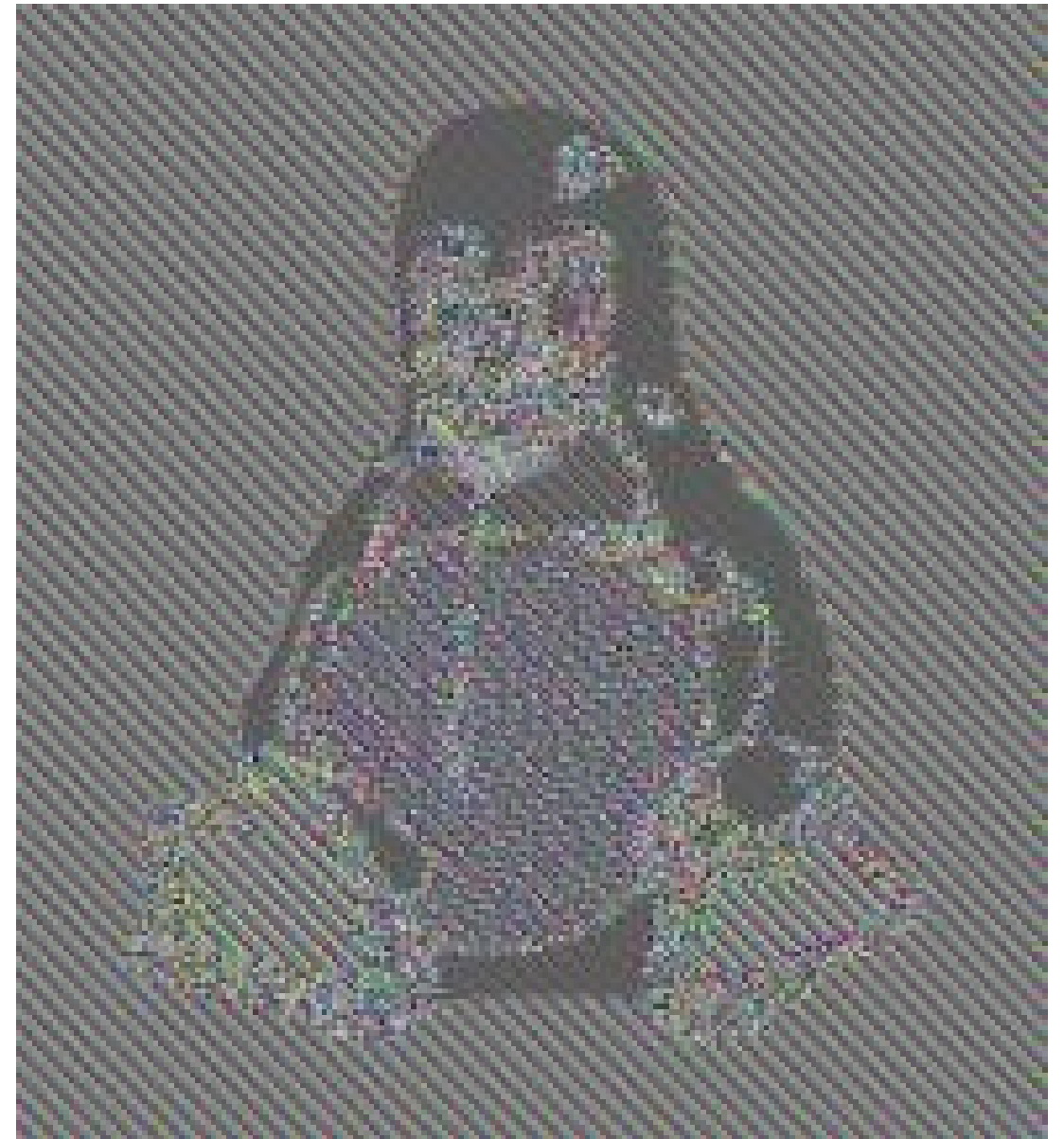
Как зашифровать
несколько блоков?

ECB

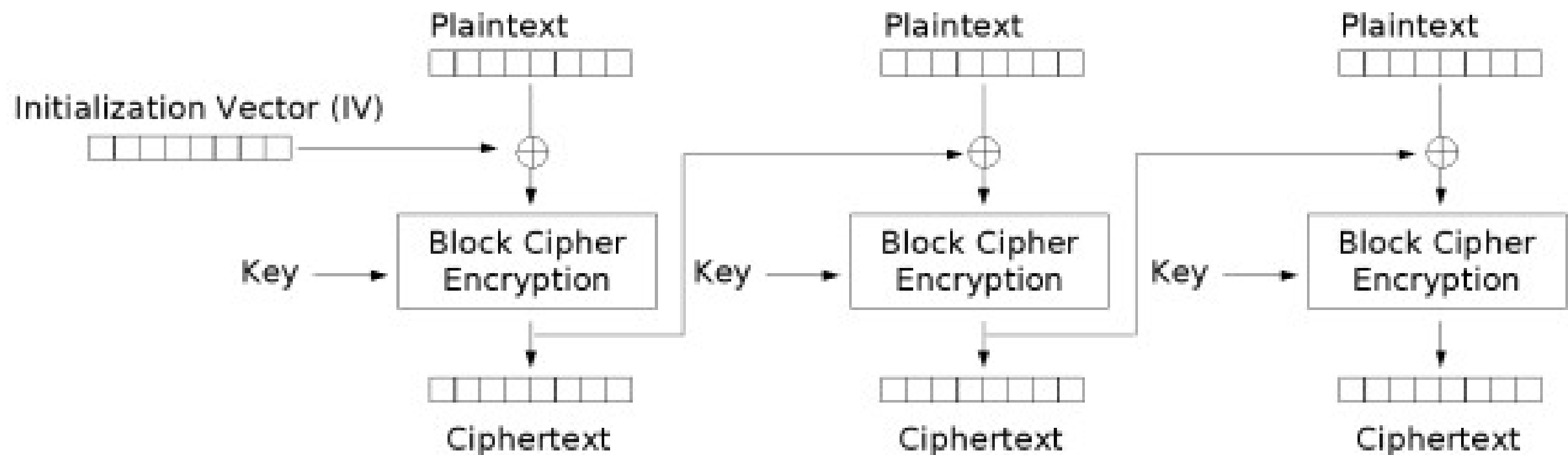


Electronic Codebook (ECB) mode encryption

ECB



CBC

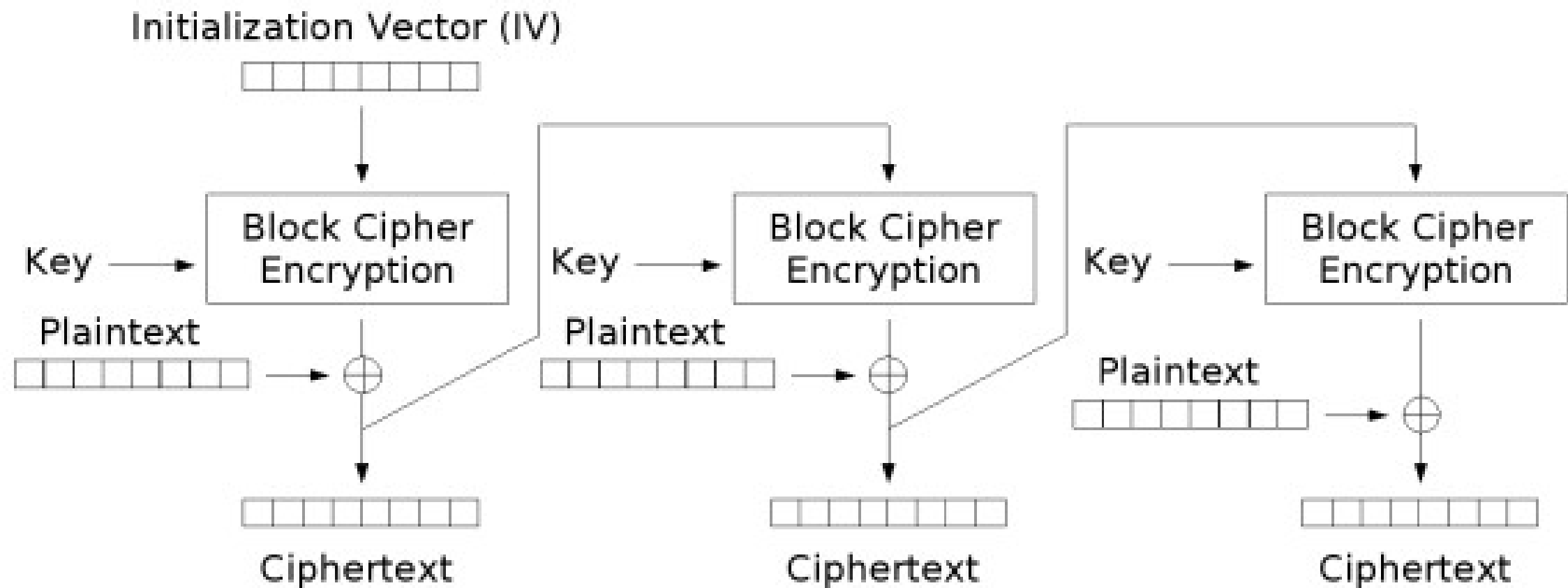


Cipher Block Chaining (CBC) mode encryption

Birthday paradox

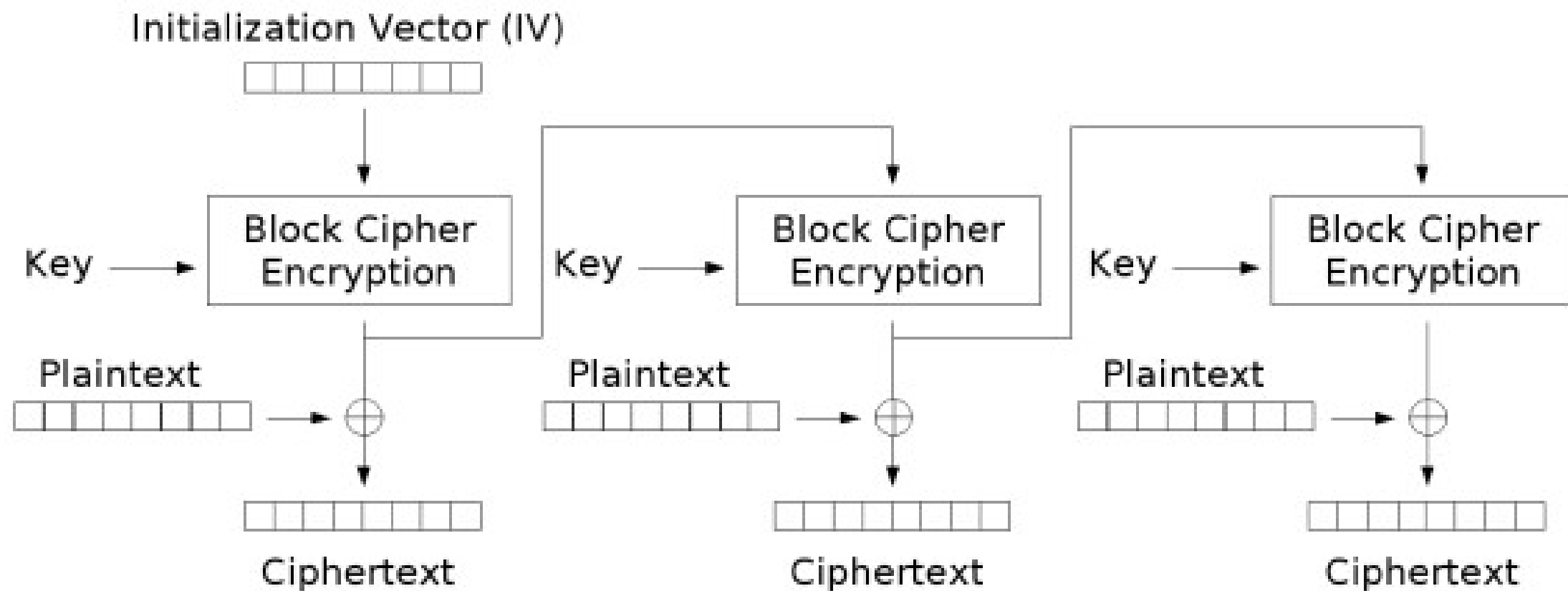
- Какова вероятность совпадения двух блоков выхода шифра?
- Как это влияет на безопасность криптосистемы?
- Сколько времени это займет на реальном трафике?

CFB



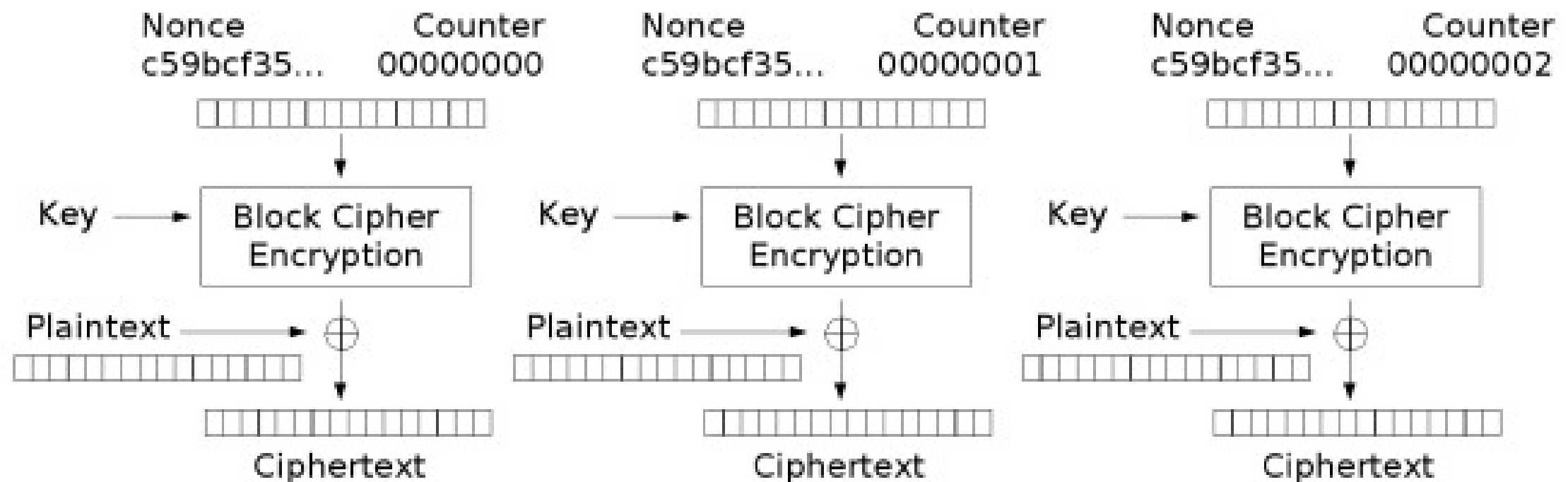
Cipher Feedback (CFB) mode encryption

OFB



Output Feedback (OFB) mode encryption

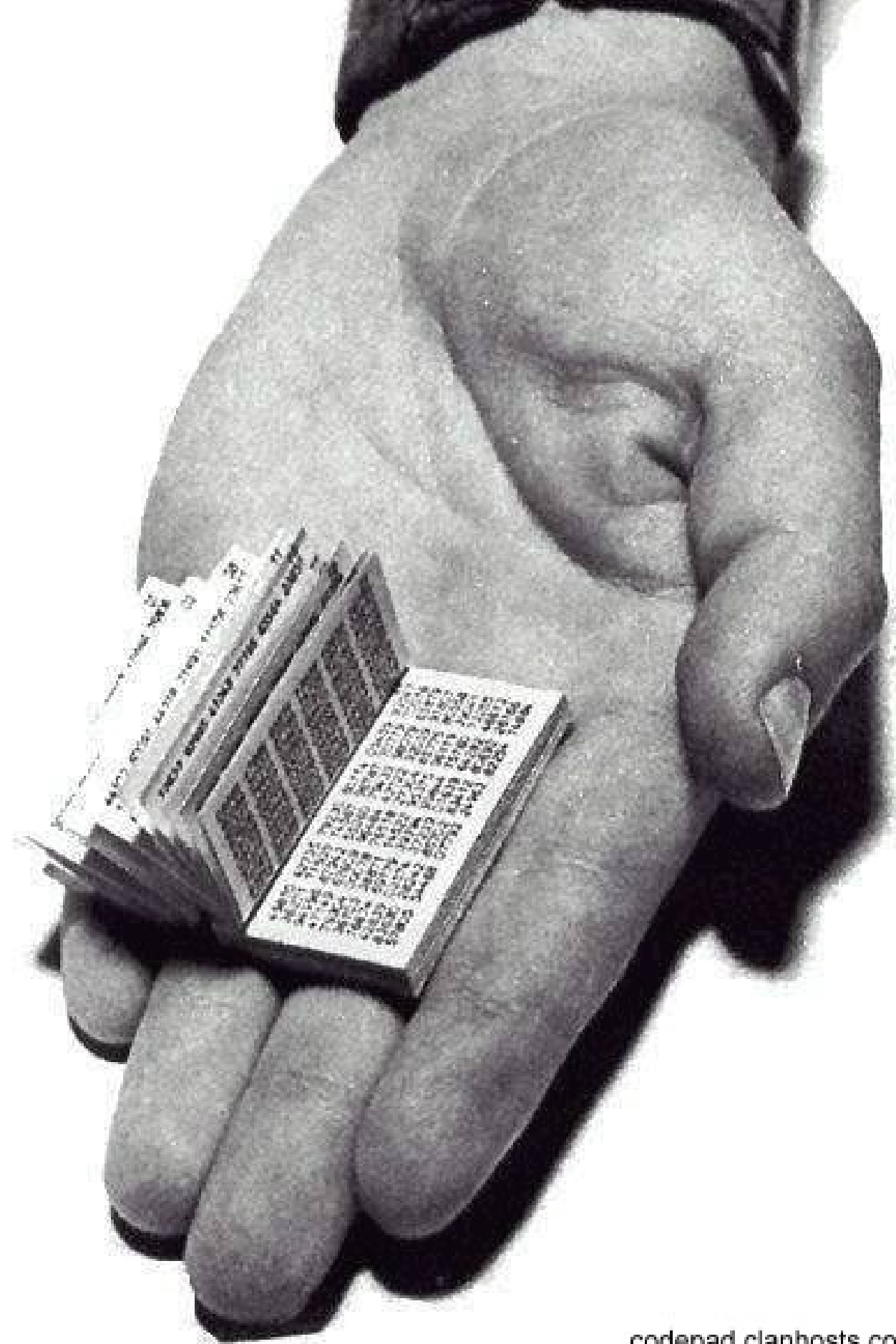
CTR



Counter (CTR) mode encryption

Потоочные шифры

- Понятие *гаммы*
- Шифр Вернама



codepad.clanhosts.com